REMARKS

The specification and claims have been amended to more clearly define the invention.

A marked-up version of the claims as amended is attached hereto entitled "VERSION WITH MARKINGS TO SHOW CHANGES MADE."

It is believed that the claims, as amended, are in condition for continued examination on the merits. Should the Examiner deem that any further action by Applicants would be desirable to place the application in better condition for allowance, the Examiner is encouraged to telephone Applicant's undersigned attorney.

The Commissioner is authorized to charge our Deposit Account No. 01-2340 for any fee which is deemed by the Patent and Trademark Office to be required to effect consideration of this statement.

Respectfully submitted,
ARMSTRONG, WESTERMAN, HATTORI,
McLELAND & NAUGHTON, LLP

for John P. Kong
Attorney for Applicant
Registration No. 40,054

Reg. No. 32,861

Attorney Docket No. **010321**
1725 K Street, N.W., Suite 1000
Washington, D.C. 20006
Tel: (202) 659-2930
JPK/nrp
Enclosure: VERSION WITH MARKINGS TO SHOW CHANGES MADE

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Please replace the paragraph beginning at page 13, line 7, with the following rewritten paragraph:

--In the description of the above embodiment, the encryption unit 20 and the decryption unit 21 are contained in the changeable key encryption/decryption unit 19 and the encryption unit 16 and the [encryption] decryption unit 17 are contained in the unchangeable key encryption/decryption unit 15. Of course, it goes without saying that these units 16, 17, 20 and 21 may also be separately provided..--

Please replace the paragraph beginning at page 14, line 21, with the following rewritten paragraph:

--In a case where the decrypted data M, for which copyrights are claimed, is stored in an external device 38, i.e., in a medium such as a digital versatile disk (DVD) RAM or a hard disk, etc., or is transferred externally via a network, the decrypted data M is re-encrypted using the unchangeable key K0 at the encryption unit 36 of the unchangeable key encryption/decryption unit 35: $\forall 0{:}C0=E(M, K0)$

$=E(D(C1, K1), K0)$,

further, the [decrypted data M] re-encrypted data C0 is double re-encrypted at an encryption unit 40 of the changeable key encryption/decryption unit 39 by using the second changeable key K2:

$\forall 0\text{-}2{:}C0\text{-}2=E(C0, K2)$

VERSION WITH MARKINGS TO SHOW CHANGES MADE

=E (E (D (C1, K1), K0), K2),

and double re-encrypted data C0-2 is stored in the external device 38 or transferred.--

Please replace the paragraph beginning at page 15, line 11 with the following rewritten paragraph:

-- In a case where the double re-encrypted data C0-2 is used again, the re-encrypted data C0-2 read from the storage medium of the external device 38 or transferred from the network is re-decrypted using the external changeable key K2 by the re-decryption unit 41 of the external changeable key encryption/decryption unit 39:

$\exists$:0:C0 = [E] D (C0-2, K2)

=D (E (E (D (C1, K1), K0), K2),

further, the re-decrypted data C0 is again re-decrypted using the unchangeable key K0 by a decryption unit 37 of the unchangeable key encryption/decryption unit 35:

$\exists$:M = D (C0, K0)

=D (E (D (C1, K1), K0)

and the decrypted data M is outputted to the display unit 34 or the like.--

Please replace the paragraph beginning at page 16, line 5, with the following rewritten paragraph:

--As described above, because the re-encryption is performed using the [second changeable] unchangeable key [K2] K0 before the re-encryption using the [unchangeable] second

changeable key [K0] K2, even when the unchangeable key K0 is discovered by others, since the data is also encrypted by using the second changeable key [K0] K2, it is very difficult to cryptanalyze the encrypted data without further finding out the second changeable key [K0] K2.--

Please replace the paragraph beginning at page 16, line 14, with the following rewritten paragraph:

--In the description of this embodiment, the encryption unit 36 and the decryption unit 37 are contained in the unchangeable key encryption/decryption unit 35 and the encryption unit 40 and the [encryption] decryption unit 41 are contained in the changeable key encryption/decryption unit 39. Of course, it goes without saying that these units 36, 37, 40 and 41 may also be separately provided.--

Please replace the paragraph beginning at page 20, line 17, with the following rewritten paragraph:

--The operating system 51 comprises an operating system service 52 and a system service API 53, which are user regions, and a kernel 54 and a HAL 55, which are non-user regions. The system service API 53 is arranged between the operating system service 52 and the kernel 54 and serves to mediate between the operating system service 52 and the kernel 54. The HAL 55 is arranged at the lowermost layer of the operating system [50] 51 and serves to absorb differences in the hardware for the software.--

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please replace the paragraph beginning at page 22, line 13, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 is utilized, the double re-encrypted data C2-0 read from the storage medium or transferred via the network is re-decrypted using the unchangeable key K0 at the unchangeable key encryption/decryption unit 57:

$\exists 2{:}C2 = [E]\ D\ (C2\text{-}0, K0)$

$= D\ (E\ (E\ (D\ (C1, K1), K2), K0).$

Further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the HAL 55 having the changeable key encryption/decryption function:

$\exists{:}M = D\ (C2, K2)$

$= D\ (E\ (D\ (C1, K1), K2),$

and the decrypted data M thus obtained is outputted to the display unit 56 or the like.--

Please replace the paragraph beginning at page 25, line 12, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 is utilized again, the double re-encrypted data C2-0 read from the storage medium or transferred via the network is re-decrypted using the unchangeable key K0 at the internal unchangeable key encryption/decryption unit 57:

$\exists 2{:}C2=[E]\ D\ (C2\text{-}0, K0)$

$=D\ (E\ (E\ (D\ (C1, K1), K2), K0).$

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Further, the re-decrypted data C2 is decrypted by the filter driver 66A or 66B, using the second changeable key K2:

$$\exists: M = D(C2, K2)$$

$$= D(E(D(C1, K1), K2)$$

and the decrypted data M thus obtained is outputted to the display unit 56 or the like. --

Please replace the paragraph beginning at page 26, line 1, with the following rewritten paragraph:

--The filter driver can be easily placed into the kernel of the operation system in a part of the I/O manager. In so doing, the function of the re-encryption/re-decryption processing and the key management can be easily incorporated into the operation system. Also, since re-encryption is performed using the second changeable key K2 before the re-encryption using the unchangeable key K0, even if the unchangeable key K0 is discovered by others, it is very difficult to cryptanalyze the encrypted data without finding out the second changeable key [K0] K2 because the data is also encrypted by the second changeable key [K0] K2.--

Please replace the paragraph beginning at page 26, line 8, with the following rewritten paragraph:

--Further, because the second changeable key [K0] K2 is used first, and is then, used after the unchangeable key K0 is used, the key security can be highly ensured. Also, because the second changeable key K2 is used first, it strongly governs the encrypted data.--

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please replace the paragraph beginning at page 26, line 13, with the following rewritten paragraph:

--In a fifth embodiment shown in Fig. 7, the changeable key encryption/decryption and the key management is provided by software carried out at the disk driver [57] 67 and the network driver 68 contained in the I/O management micro-kernel 64 in the operating system 51.--

Please replace the paragraph beginning at page 28, line 1, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 is utilized again, the double re-encrypted data C2-0 read from the storage medium or transferred via a network is re-decrypted using the unchangeable key K0 by the internal unchangeable key encryption/decryption unit 57:

$\exists 2: C2 = [E] D (C2\text{-}0, K0)$

$= D (E (E (D (C1, K1), K2), K0).$

Further, the re-decrypted data C2 is decrypted by the device driver 71, i.e., the disk driver 67 and the network driver 68, using the second changeable key K2:

$\exists: M = D (C2, K2)$

$= D (E (D (C1, K1), K2)$

and the decrypted data M thus obtained is outputted to the display unit 56 or the like.--

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please replace the paragraph beginning at page 31, line 14, with the following rewritten paragraph:

--When the re-encrypted data C2-0 stored in the storage medium 81 is utilized, the double re-encrypted data C2-0 read from the storage medium 81 is decrypted using the unchangeable crypt key K0 placed in a decryption unit 17 of the internal unchangeable key encryption/decryption unit 15:

$$\exists 2: C2 = D(C2\text{-}0, K0)$$
$$= D(E(E(D(C1, K1), K2), K0)$$
$$= E(E(D(C1, K1), K2),$$

further, the re-decrypted data C2 is decrypted using the changeable key K2 by a decryption unit 21 of the changeable key encryption/decryption unit 19:

$$\exists: M = D(C2, K2)$$
$$= D(E(D(C1, K1), K2)$$

and the decrypted data M is outputted to the display unit 14 or the like.--

Please replace the paragraph beginning at page 32, line 4, with the following rewritten paragraph:

--In this case, in order to ensure security, when the double re-encrypted data C2-0 is read from the storage medium 81 via a path shown by a broken line in the figure, it may be designed in a manner that the double re-encrypted data C2-0 in the storage medium 81 is erased at that

time, and that the data re-encrypted using the changeable key K2 and the internal unchangeable key K0 is stored again.--

Please replace the paragraph beginning at page 35, line 12, with the following rewritten paragraph:

--In this case, in order to ensure security, when the double re-encrypted data C0-2 is read from the storage medium 81 via a route shown by a broken line in the figure, it may be designed in a manner that the double re-encrypted data C0-2 in the storage medium 81 is erased at that time, and that the data re-encrypted using the second changeable key K2 and the unchangeable key K0 is stored again.--

Please replace the paragraph beginning at page 36, line 8, with the following rewritten paragraph:

--When the double re-encrypted data C3-2 sent to the externals 82 is utilized, the double re-encrypted data C3-2 is decrypted using the [third] second changeable key [K3] K2 by the decryption unit 84 of the changeable key encryption/decryption unit 83:

$\exists 3$: C3 = D (C3-2, K2)

= D (E (C3, K2), K2),

further, the re-encrypted data [C2] C3 thus obtained is decrypted using the third changeable key K3 by the decryption unit 85 of the changeable key encryption/decryption unit 83:

$\exists$: M = D (C3, K3)

= D (E (M, K3), K3)

and the decrypted data M thus obtained is outputted to the display unit 86 or the like.--

Please replace the paragraph beginning at page 37, line 17, with the following rewritten paragraph:

--For this purpose, changeable key encryption units 90 and 91 are provided as hardware 88, in addition to the unchangeable key encryption/decryption unit 89. In a case where the copyrighted and decrypted data is stored in the hard disk 81 of the storage medium incorporated in or dedicated to the computer, it is double re-encrypted and decrypted using the unchangeable key K0 by the encryption/decryption unit [91] 89 via a disk driver 67. In a case where the data is stored in the DVD-RAM [89] 92 of the removable medium, it is double re-encrypted and decrypted using the third changeable key K3 by the encryption/ decryption unit 90 via the disk driver 67. In a case where the data is transferred externally via the network 93, it is double re-encrypted and decrypted using the third changeable key K3 by the changeable key encryption/decryption unit 91 via a network driver 68.--

Please replace the paragraph beginning at page 39, line 6, with the following rewritten paragraph:

--In a case where the double re-encrypted data C2-0 stored in the storage medium 81 is utilized, the double re-encrypted data C2-0 read from the storage medium 81 is re-decrypted using the unchangeable key K0 by the encryption/decryption unit 89 in the hardware 88:

∃2: C2 = [E] D (C2-0, K0) =D (E (E (D (C1, K1), K2), K0),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the filter driver 66 having encryption/ decryption function:

$\exists$: M=D (C2, K2) =D (E (D (C1, K1), K2),

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.--

Please replace the paragraph beginning at page 39, line 15, with the following rewritten paragraph:

--When the re-encrypted data C2 is stored in a DVD-RAM of the removable medium, the re-encrypted data C2 is double re-encrypted using the [second] third changeable key [K2] K3 by the changeable key encryption/decryption unit 90 of the hardware:

$\forall$2-3: C2-3=E (C2, K3) =E (E (D (C1, K1), K2), K3)

and double re-encrypted data C2-3 is stored in the removable medium, the DVD-RAM.--

Please replace the paragraph beginning at page 43, line1, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 stored in the storage medium 81 is utilized, the double re-encrypted data C2-0 read from the storage medium 81 is re-decrypted using the unchangeable key K0 by the encryption/decrypted unit 89 in the hardware 88:

$\exists$2: C2 = [E] D (C2-0, K0) =D (E (E (D (C1, K1), K2), K0),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the filter driver 66 having encryption/decryption function:

$\exists$: M = D (C2, K2) =D (E (D (C1, K1), K2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.--

Please replace the paragraph beginning at page 43, line 16, with the following rewritten paragraph:

--When the double re-encrypted data C2-3 stored in the removable medium 92 is utilized, the re-encrypted data C2-3 read from the removable medium 92 is re-decrypted using the third changeable key K3 by the encryption/decryption unit 90 in the hardware 88:

$\exists$2: C2 = [E] D (C2-3, K3) =D (E (E (D (C1, K1), K2), K3),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the filter driver 66 having encryption/decryption function:

$\exists$: M = D (C2, K2) =D (E (D (C1, K1), K2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.--

Please replace the paragraph beginning at page 47, line 3, with the following rewritten paragraph:

VERSION WITH MARKINGS TO SHOW CHANGES MADE

--In Fig. 12, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive [105] 106, a CD-ROM drive 107, a modem 108, etc. are connected to a system-bus 102 connected to the CPU 101.--

Please replace the paragraph beginning at page 47, line 19, with the following rewritten paragraph:

--In cases where the decrypted digital data M is stored in the hard disk drive 105, where it is copied at the flexible disk drive [105] 106 or where it is transferred via the modem 108, the decrypted digital data is re-encrypted using the second changeable key K2 by the [re-encryption] encryption unit [115] 112:

$$\forall 2: C2 = E(M, K2)$$

$$= E(D(C1, K1), K2),$$

the re-encrypted digital data C2 is supplied to the system-bus 102, and is stored in the hard disk drive 105, copied in the flexible disk drive [105] 106 or transferred via the modem 108.

Please replace the paragraph beginning at page 49, line 7, with the following rewritten paragraph:

--In Fig. 13, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive [105] 106, a CD-ROM drive 107, a modem 108, etc. are connected to a system-bus 102 connected to the CPU 101.--

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please replace the paragraph beginning at page 51, line 8, with the following rewritten paragraph:

--When the decrypted digital data M is stored at the hard disk drive 105 or is copied at the flexible disk drive [105] 106 or is transferred via the modem 108, it is re-encrypted using the second changeable key K2 by the [re-encryption] encryption unit [115] 112:

$\forall$=2: C2 = E (M, K2)

= E (D (C1, K1), K2),

the re-encrypted digital data C2 is supplied to the system-bus 102, and it is stored at the hard disk drive 105, copied at the flexible disk drive [105] 106, or transferred via the modem 108.--

Please replace the paragraph beginning at page 52, line 5, with the following rewritten paragraph:

--When the encrypted audio signal Ca0 is inputted to the encrypted audio data player 126 from the crypt audio interface 123, it is decrypted using the unchangeable key K0 by the unchangeable key decryption unit 129:

Ma=D (Ca0, K0),

the decrypted audio signal [MA] Ma is converted to a playable analog signal by the D/A converter 132, and it is played by the speaker [116] 117.--

Please replace the paragraph beginning at page 53, line 8, with the following rewritten paragraph:

VERSION WITH MARKINGS TO SHOW CHANGES MADE

--In Fig. 14, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive [105] 106, a CD-ROM drive 107, a modem 108, etc., are connected to a system-bus 102 connected to the CPU 101.--

Please replace the paragraph beginning at page 53, line 11, with the following rewritten paragraph:

--Reference numeral 140 represents a copyright management apparatus, which comprises a decryption/[re-]encryption unit 110, a video interface 113, an audio interface 114, a printer interface 141, and an unchangeable key encryption unit 134.--

Please replace the paragraph beginning at page 53, line 14, with the following rewritten paragraph:

--The decryption/[re-]encryption unit 110 has a decryption unit 111 and an re-encryption unit 112.--

Please replace the paragraph beginning at page 53, line 16, with the following rewritten paragraph:

--The unchangeable key encryption unit 134 has an unchangeable key encryption unit for video [142] 135, an unchangeable key encryption unit for audio 136, and an unchangeable key encryption unit for print 137. The unchangeable key encryption units for video, audio and print may be arranged in a single unit if it is available for sufficient encryption capacity.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please replace the paragraph beginning at page 53, line 20, with the following rewritten paragraph:

--The decryption unit 111 and the re-encryption unit 112 of the decryption/encryption unit 110 are connected to the system-bus 102 of the computer. Further, the video interface [113] 131, the audio interface [114] 132 and the printer interface [115] 133 are connected to the decryption unit 111, and the unchangeable key encryption unit for video 135, the unchangeable key encryption unit for audio 136 and the unchangeable key encryption unit for print 137 are connected to these interfaces.--

Please replace the paragraph beginning at page 54, line 7, with the following rewritten paragraph:

--The above arrangement can be easily realized by designing the copyright management apparatus [120] 140 as a sub-computer arrangement having a CPU and a system-bus.

Please replace the paragraph beginning at page 55, line 5, with the following rewritten paragraph:

--When the decrypted digital data M is stored at the hard disk drive 105 or copied at the flexible disk drive [105] 106 or transferred via the modem 108, it is re-encrypted using the second changeable key K2 by the [re-]encryption unit [115] 112:

$\forall 2$: C2=E (M, K2)

=E (D (C1, K1), K2),

the re-encrypted digital data C2 is supplied to the system-bus 102, and it is then stored at the hard disk drive 105, copied at the flexible disk drive [105] 106 or transferred via the modem 108.

Please replace the paragraph beginning at page 55, line 12, with the following rewritten paragraph:

--When the decrypted digital data M is outputted to the encrypted data display unit 125, the encrypted audio data player 126 or the encrypted data printer 127, the decrypted digital data M is arranged to digital data Md, Ma and Mp to be provided to the display unit 116, the speaker 117 and the printer 118 respectively at the video interface 131, the audio interface 132 and the printer interface 133 in the copyright management apparatus [120] 140. Then, these digital data are encrypted using the unchangeable key K0 by the unchangeable key encryption unit for video 135, the unchangeable key encryption unit for audio 136 and the unchangeable key encryption unit for print 137:

Cd0=E (Md, K0)

Ca0=E (Ma, K0)

Cp0=E (Mp, K0)

and the encrypted display signal Cd0, the encrypted audio signal Ca0 and the encrypted print signal Cp0 are outputted.--

Please replace the paragraph beginning at page 56, line 17, with the following rewritten paragraph:

VERSION WITH MARKINGS TO SHOW CHANGES MADE

--The encrypted print signal Cp0 is inputted to the encrypted data printer 127 from the unchangeable key encryption unit 137, and it is decrypted using the unchangeable key K0:

Mp=D (Cp0, K0).

The decrypted [audio] print signal Mp is printed by the printer 118..--

Please replace the paragraph beginning at page 56, line 21, with the following rewritten paragraph:

--When this copyright management apparatus 140 is used, no decrypted data is present outside the copyright management apparatus [120] 140.--

IN THE CLAIMS:

1. (Amended) A method for protecting decrypted digital data[, to which encrypted digital data is decrypted,] from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said method comprising the steps of:

encrypting said decrypted digital data [by] using a changeable key to produce changeable key re-encrypted digital data [re-encrypted by the changeable key];

encrypting said changeable key re-encrypted digital data [re-encrypted by the changeable key by] using an unchangeable key in a device to produce changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by changeable-unchangeable keys] to be stored, copied or transferred;

decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by changeable-unchangeable keys, by] using said unchangeable key to said changeable key re-encrypted digital data [re-encrypted by the changeable key]; and

decrypting said changeable key re-encrypted digital data [re-encrypted by the changeable key, by] using said changeable key to said decrypted digital data.

2. (Amended) A method for protecting decrypted digital data[, to which encrypted digital data is decrypted,] from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, comprising the steps of:

encrypting said decrypted digital data [by] using an unchangeable key in a device to produce unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key];

encrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using a changeable key to produce unchangeable-changeable keys double re-encrypted digital data [double re-encrypted by changeable-unchangeable keys] to be stored, copied or transferred;

decrypting said copied, stored or transferred unchangeable-changeable keys double re-encrypted digital data [double re-encrypted by changeable-unchangeable keys, by] using said changeable key to said unchangeable key re-encrypted digital data [re-encrypted by the changeable key]; and

VERSION WITH MARKINGS TO SHOW CHANGES MADE

decrypting said unchangeable key re-encrypted digital data [decrypted by the changeable key, by] using said unchangeable key to said decrypted digital data.

3. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting [by] using said changeable key are carried out by a software.

4. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting [by] using said changeable key are carried out by a hardware.

5. (Amended) The method according to claim 1 or 2, wherein said changeable key is supplied externally from [the outside of a] said device.

6. (Amended) The method according to claim 1 or 2, wherein said changeable key is generated in [a] said device.

7. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a software.

8. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a hardware.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

9. (Amended) The method according to claim 1 or 2, wherein said unchangeable key is already placed in said device.

10. (Amended) The method according to claim 1 or 2, wherein said unchangeable key is generated in said device.

11. (Amended) The method according to claim 1 or 2, wherein said unchangeable key is supplied externally from [the outside of] said device.

12. (Amended) The method according to claim 9, 10 or 11, wherein said unchangeable key is specific to said device.

13. (Amended) The method according to claim 9, 10 or 11, wherein said unchangeable key is not specific to said device.

14. (Amended) An apparatus for protecting decrypted digital data[, to which encrypted digital data is decrypted,] from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising:

a changeable key [re-encryption] encryption unit for encrypting said decrypted digital data [by] using a changeable key to produce changeable key re-encrypted digital data [re-encrypted];

an unchangeable key encryption unit for encrypting said changeable key re-encrypted digital data [re-encrypted by the changeable key by] using an unchangeable key in a device to

produce changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by changeable-unchangeable keys] to be stored, copied or transferred;

an unchangeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by changeable-unchangeable keys, by] using said unchangeable key to said changeable key re-encrypted digital data [re-encrypted by the unchangeable key]; and

a changeable key decryption unit for decrypting said changeable key re-encrypted digital data [re-encrypted by the unchangeable key, by] using said changeable key to said decrypted digital data.

15. (Amended) An apparatus for protecting decrypted digital data[, to which encrypted digital data is decrypted,] from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data [by] using an unchangeable key in a device to produce unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key];

a changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using a changeable key to produce changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by changeable-unchangeable keys] to be stored, copied or transferred;

a changeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by

changeable-unchangeable keys, by] using said changeable key to said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key]; and

an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key, by] using said unchangeable key to said decrypted digital data.

16. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting [by] using said changeable key are carried out by a software.

17. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting [by] using said changeable key are carried out by a hardware.

18. (Amended) The apparatus according to claim 14 or 15, wherein said changeable key is supplied externally from [the outside of a] said device.

19. (Amended) The apparatus according to claim 14 or 15, wherein said changeable key is generated in [a] said device.

20. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting [by] using said unchangeable key are carried out by a software.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

21. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting [by] using said unchangeable key are carried out by a hardware.

22. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is already placed in said device.

23. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is generated in said device.

24. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is supplied <u>externally</u> from [the outside of] said device.

25. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is specific to said device.

26. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is not specific to said device.

27. (Amended) A method for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, <u>said decrypted digital data being decrypted from digital data encrypted using a first changeable key,</u> said method comprising the steps of:

encrypting said decrypted digital data [by] using a second changeable key to produce second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data [double re-encrypted by unchangeable-second-changeable keys] to be stored;

decrypting said stored unchangeable-second changeable keys double re-encrypted digital data [double re-encrypted by unchangeable-second-changeable keys by] using said unchangeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys] to be copied or transferred;

decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data double [re-encrypted by third-changeable-second-changeable keys by] using said third changeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key]; and

decrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using said second changeable key to said decrypted digital data.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

28. (Amended) A method for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of:

encrypting said decrypted digital data [by] using a second changeable key to produce second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data [double re-encrypted by unchangeable-second-changeable keys] to be stored;

decrypting said stored unchangeable-second changeable keys double re-encrypted digital data double [re-encrypted by unchangeable-second-changeable keys by] using said unchangeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys] to be copied or transferred;

decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data double [re-encrypted by third-changeable-second-changeable keys by]

using said third changeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key]; and

decrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using said second changeable key to said decrypted digital data.

29. (Amended) A method for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of:

encrypting said decrypted digital data [by] using an unchangeable key in a device to produce unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key], and encrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data double [re-encrypted by second-changeable-unchangeable keys] to be stored;

decrypting said stored second changeable-unchangeable keys double re-encrypted digital data double [re-encrypted by second-changeable-unchangeable keys by] using said second changeable key to said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key];

decrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using said unchangeable key to said decrypted digital data;

VERSION WITH MARKINGS TO SHOW CHANGES MADE

encrypting said [re-encrypted] decrypted digital data [by] using a third changeable key to produce third changeable key re-encrypted digital data [re-encrypted by the third changeable key], and encrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key] using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys] to be copied or transferred;

decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys by] using said second changeable key to said third changeable key re-encrypted digital data [re-encrypted by the third changeable key]; and

decrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key by] using said third changeable key to said decrypted digital data.

30. (Amended) A method for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of:

encrypting said decrypted digital data [by] using an unchangeable key in a device to produce unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key], and encrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using a second changeable key to produce second changeable-unchangeable keys double

re-encrypted digital data [double re-encrypted by second-changeable-unchangeable keys to be stored];

decrypting said stored second changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by second-changeable-unchangeable keys by] using said second changeable key to said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key];

decrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using said unchangeable key to said decrypted digital data;

encrypting said [re-encrypted] decrypted digital data [by] using a third changeable key to produce third changeable key re-encrypted digital data [re-encrypted by the third changeable key], and encrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key] using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys] to be copied or transferred;

decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys by] using said second changeable key to said third changeable key re-encrypted digital data [re-encrypted by the third changeable key]; and

decrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key by] using said third changeable key to said decrypted digital data.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

31. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting [by] using said second changeable key are carried out by a software.

32. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting [by] using said second changeable key are carried out by a hardware.

33. (Amended) The method according to claim 27, 28, 29 or 30, wherein said second changeable key is supplied externally from [the outside of a] said device.

34. (Amended) The method according to claim 27, 28, 29 or 30, wherein said second changeable key is generated in [a] said device.

35. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting [by] using said third changeable key are carried out by a software.

36. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting [by] using said third changeable key are carried out by a hardware.

37. (Amended) The method according to claim 27, 28, 29 or 30, wherein said third changeable key is supplied externally from [the outside of a] said device.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

38. (Amended) The method according to claim 27, 28, 29 or 30, wherein said third changeable key is generated in [a] said device.

39. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a software.

40. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a hardware.

41. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is already placed in said device.

42. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is generated in said device.

43. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is supplied externally from [the outside of] said device.

44. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is specific to [a] said device.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

45. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is not specific to [a] said device.

46. (Amended) An apparatus for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data [by] using a second changeable key to produce second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

an unchangeable key encryption unit for encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data [double re-encrypted by unchangeable-second-changeable keys] to be stored;

an unchangeable key decryption unit for decrypting said stored unchangeable-second changeable keys double re-encrypted digital data [double re-encrypted by unchangeable-second-changeable keys by] using said unchangeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

a third changeable key encryption unit for encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using a third changeable

key to produce third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys] to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys by] using said third changeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key]; and

a second changeable key decryption unit for decrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using said second changeable key to said decrypted digital data.

47. (Amended) An apparatus for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data [by] using a second changeable key to produce second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

an unchangeable key encryption unit for encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data [double re-encrypted by unchangeable-second-changeable keys] to be stored;

VERSION WITH MARKINGS TO SHOW CHANGES MADE

an unchangeable key decryption unit for decrypting said stored unchangeable-second changeable keys double re-encrypted digital data [double re-encrypted by unchangeable-second-changeable keys by] using said unchangeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key];

a third changeable key encryption unit for encrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys] to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys by] using said third changeable key to said second changeable key re-encrypted digital data [re-encrypted by the second changeable key]; and

a second changeable key decryption unit for decrypting said second changeable key re-encrypted digital data [re-encrypted by the second changeable key by] using said second changeable key to said decrypted digital data.

48. (Amended) An apparatus for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

VERSION WITH MARKINGS TO SHOW CHANGES MADE

an unchangeable key encryption unit for encrypting said decrypted digital data [by] using an unchangeable key in a device to produce unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key], and a second changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by second-changeable-unchangeable keys] to be stored;

a second changeable key decryption unit for decrypting said stored second changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by second-changeable-unchangeable keys by] using said second changeable key to said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key], and an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using said unchangeable key to said decrypted digital data;

a third changeable key encryption unit for encrypting said [re-encrypted] decrypted digital data [by] using a third changeable key to produce third changeable key re-encrypted digital data [re-encrypted by the third changeable key], and a second changeable key encryption unit for encrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key] using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys] to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys by] using said second changeable key to said third changeable key re-encrypted digital data [re-encrypted by the third changeable key], and a third changeable key decryption unit for decrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key by] using said third changeable key to said decrypted digital data.

49. (Amended) An apparatus for protecting decrypted digital data[, to which digital data encrypted by a first changeable key is decrypted,] from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data [by] using an unchangeable key in a device to produce unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key], and a second changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by second-changeable-unchangeable keys] to be stored;

a second changeable key decryption unit for decrypting said stored second changeable-unchangeable keys double re-encrypted digital data [double re-encrypted by

second-changeable-unchangeable keys by] using said second changeable key to said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key], and an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data [re-encrypted by the unchangeable key by] using said unchangeable key to said decrypted digital data;

a third changeable key encryption unit for encrypting said [re-encrypted] decrypted digital data [by] using a third changeable key to produce third changeable key re-encrypted digital data [re-encrypted by the third changeable key], and a second changeable key encryption unit for encrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key] using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys] to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data [double re-encrypted by second-changeable-third-changeable keys by] using said second changeable key to said third changeable key re-encrypted digital data [re-encrypted by the third changeable key], and a third changeable key decryption unit for decrypting said third changeable key re-encrypted digital data [re-encrypted by the third changeable key by] using said third changeable key to said decrypted digital data.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

50. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting [by] using said second changeable key are carried out by a software.

51. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting [by] using said second changeable key are carried out by a hardware.

52. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is supplied externally from [the outside of a] said device.

53. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is generated in [a] said device.

54. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting [by] using said third changeable key are carried out by a software.

55. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting [by] using said third changeable key are carried out by a hardware.

56. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is supplied externally from [the outside of a] said device.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

57. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is generated in [a] said device.

58. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a software.

59. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a hardware.

60. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is already placed in the device.

61. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is generated in the device.

62. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is supplied externally from [the outside of] the device.

63. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is specific to said device.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

64. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is not specific to said device.

65. (Amended) A method for protecting digital data from illegitimate use, said method comprising the steps of:

determining whether said digital data is subject to be protected or not;

encrypting said digital data, determined [being subject] to be protected, [by] using an unchangeable key in [said] a device to produce unchangeable key encrypted digital data [encrypted by the unchangeable key];

storing, copying or transferring said unchangeable key encrypted digital data [determined being not subject to be protected and said digital data encrypted by the unchangeable key];

decrypting said stored, copied or transferred unchangeable key encrypted digital data [encrypted by the unchangeable key by] using said unchangeable key to said decrypted digital data; and

utilizing said stored, copied or transferred unchangeable key encrypted digital data and said decrypted digital data.

66. (Amended) The method according to claim 65, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a software.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

67. (Amended) The method according to claim 65, wherein said steps of encrypting and decrypting [by] using said unchangeable key are carried out by a hardware.

68. (Amended) The method according to claim 65, in which encrypting and decrypting [by] using said unchangeable key are controlled by identifying information which is added to said digital data.

69. (Amended) The method according to claim 68, in which encrypting and decrypting are carried out [by presence of] <u>when</u> said identifying information <u>is present</u>.

70. (Amended) The method according to claim 68, in which encrypting and decrypting are carried out [by absence of] <u>when</u> said identifying information <u>is absent</u>.

71. (Amended) The method according to claim 65, wherein said unchangeable key is already placed in [a] <u>said</u> device.

72. (Amended) The method according to claim 65, wherein said unchangeable key is generated in the device.

73. (Amended) The method according to claim 65, wherein said unchangeable key is supplied <u>externally</u> from [the outside of] the device.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

74. (Amended) The method according to claim 71, 72 or 73, wherein said unchangeable key is specific to the device.

75. (Amended) The method according to claim 71, 72 or 73, wherein said unchangeable key is not specific to the device.

76. (Amended) An apparatus for protecting digital data from illegitimate use, said apparatus comprising:

determining means <u>for determining</u> [as to] whether said digital data is subject to be protected or not;

means for encrypting said digital data, determined being subject to be protected, [by] using an unchangeable key in a device to <u>produce unchangeable key encrypted</u> digital data [encrypted by the unchangeable key];

means for storing, copying or transferring said <u>unchangeable key encrypted</u> digital data [determined being not subject to be protected and said digital data encrypted by the unchangeable key];

means for decrypting said stored, copied or transferred <u>unchangeable key encrypted</u> digital data [encrypted by the unchangeable key by using said unchangeable key] to <u>said</u> decrypted digital data; and

means for utilizing said stored, copied or transferred <u>unchangeable key encrypted</u> digital data and said decrypted digital data.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

77. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting [by] using said unchangeable key are carried out by a software.

78. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting [by] using said unchangeable key are carried out by a hardware.

79. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting [by] using said unchangeable key are controlled by identifying information which is added to said digital data.

80. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting are carried out [by presence of] when said identifying information is present.

81. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting are carried out [by absence of] when said identifying information is absent.

82. (Amended) The apparatus according to claim 76, wherein said unchangeable key is already placed in [a] the device.

83. (Amended) The apparatus according to claim 76, wherein said unchangeable key is generated in the device.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

84. (Amended) The apparatus according to claim 76, wherein said unchangeable key is supplied externally from [the outside of] the device.

85. (Amended) The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is specific to the device.

86. (Amended) The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is not specific to the device.